IX kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

# KANCELARIA SEJMU
# Biuro Komisji Sejmowych

## PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 22)**

z dnia 15 grudnia 2020 r.

# Pełny zapis przebiegu posiedzenia

# Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 22)

15 grudnia 2020 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Jana Grabca (KO)**, przewodniczącego Komisji, rozpatrzyła:

**– informację Ministra Cyfryzacji na temat realizacji założeń „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024";**

**– informację Ministra Cyfryzacji na temat opracowania i wdrożenia planów dotyczących przygotowania Narodowych Standardów Cyberbezpieczeństwa.**

W posiedzeniu udział wzięli: **Marek Zagórski** sekretarz stanu w Kancelarii Prezesa Rady Ministrów i pełnomocnik rządu do spraw cyberbezpieczeństwa wraz ze współpracownikami, **Adam Zakrzewski** główny specjalista w Departamencie Porządku i Bezpieczeństwa Publicznego Najwyższej Izby Kontroli, **Jacek Matyszczak** dyrektor Departamentu Bezpieczeństwa Urzędu Komunikacji Elektronicznej, **Krzysztof Zieliński** dyrektor Departamentu Cyberbezpieczeństwa Urzędu Komisji Nadzoru Finansowego, płk **Arkadiusz Ratajczak** zastępca dyrektora Departamentu I Agencji Bezpieczeństwa Wewnętrznego wraz ze współpracownikami, płk **Marcin Brzeziński** i płk **Paweł Doniec** eksperci Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, **Krzysztof Silicki** zastępca dyrektora Naukowej i Akademickiej Sieci Komputerowej, **Jacek Skrzynecki** pracownik Departamentu Cyfryzacji Urzędu Marszałkowskiego Województwa Pomorskiego, **Wiesław Paluszyński** wiceprezes Polskiej Izby Informatyki i Telekomunikacji wraz ze współpracownikami, **Magdalena Bublewicz** kierownik do spraw regulacyjnych i public affairs Związku Pracodawców Branży Internetowej IAB Polska wraz ze współpracownikami oraz **Rafał Jaczyński** ekspert Pracodawców RP.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Mariusz Pawełczyk** i **Wioletta Więciorkowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

**Przewodniczący poseł Jan Grabiec (KO):**

Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Witam, panie pośle. Witam wszystkich posłów obecnych na sali oraz uczestniczących w posiedzeniu zdalnie. Witam serdecznie gości komisyjnych – pana ministra Marka Zagórskiego z kancelarii premiera, reprezentującego dział cyfryzacji wraz z panem dyrektorem Robertem Kosibą. Witam obecnych zdalnie przedstawicieli Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, Agencji Bezpieczeństwa Wewnętrznego, Urzędu Komunikacji Elektronicznej, Naukowej i Akademickiej Sieci Komputerowej, Najwyższej Izby Kontroli, Komisji Nadzoru Finansowego, a także przedstawicieli organizacji i firm z branży cyfrowej, przedstawicieli pracodawców i samorządu.

Informuję, że posiedzenie Komisji zostało zwołane przez marszałek Sejmu na podstawie art. 198j ust. 2 regulaminu Sejmu i będzie prowadzone z wykorzystaniem środków komunikacji elektronicznej umożliwiających porozumiewanie się na odległość. Paniom i panom posłom, którzy uczestniczą w posiedzeniu zdalnie, przypominam, że zgłoszenia do zabrania głosu w dyskusji należy wysyłać pod adres e-mail <kcnt@sejm.gov.pl> lub przez czat w aplikacji Whereby po zalogowaniu się do pokoju wideokonferencyjnego. Jednocześnie informuję, że posłowie członkowie Komisji obecni na sali obrad Komisji głosują przy użyciu urządzenia do głosowania za pomocą legitymacji poselskiej. Wówczas nie logują się w systemie komunikacji elektronicznej i nie używają tabletów.

Przystępujemy teraz do stwierdzenia kworum. Bardzo proszę państwa posłów o naciśnięcie jakiegokolwiek przycisku w celu potwierdzenia obecności na posiedzeniu. Szanowni państwo, trwa potwierdzenie kworum. Za chwilę zamkniemy to głosowanie. Jeśli ktoś jeszcze z parlamentarzystów nie potwierdził obecności i swojego udziału podczas posiedzenia, to jest ostatni moment. Dobrze, zamykamy głosowanie. Bardzo proszę o podanie wyniku. Dziękuję bardzo.

Głosowało 15 członków Komisji. Stwierdzam, że mamy kworum.

Stwierdzam także przyjęcie protokołu poprzedniego posiedzenia Komisji wobec niewniesienia do niego zastrzeżeń.

Szanowni państwo, porządek dzisiejszego posiedzenia przewiduje w punkcie pierwszym informację ministra cyfryzacji na temat realizacji założeń „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024", zaś w punkcie drugim informację ministra cyfryzacji na temat opracowania i wdrożenia planów dotyczących przygotowania narodowych standardów cyberbezpieczeństwa.

Czy są uwagi do zaproponowanego porządku dziennego? Nie ma zgłoszeń. W związku z tym uważam porządek dzienny za przyjęty.

Przechodzimy do punktu pierwszego porządku dziennego, a zarazem, jak sądzę, i drugiego, bo proponuję, by łącznie rozpatrywać oba te punkty jako dotyczące tej samej problematyki. Bardzo proszę pana ministra Marka Zagórskiego, sekretarza stanu w Kancelarii Prezesa Rady Ministrów, o przedstawienie informacji. Bardzo proszę, panie ministrze.

**Sekretarz stanu w Kancelarii Prezesa Rady Ministrów i pełnomocnik rządu do spraw cyberbezpieczeństwa Marek Zagórski:**

Bardzo dziękuję. Panie przewodniczący, Wysoka Komisjo, chciałbym przedstawić krótką informację na temat realizacji założeń „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" oraz informację na temat realizacji prac nad narodowymi standardami cyberbezpieczeństwa (NSC). Rzeczywiście zrobię to łącznie. Chciałbym przede wszystkim powiedzieć, że bardzo szczegółowy materiał z realizacji tego planu przekazaliśmy na ręce pana przewodniczącego, więc pozwolę sobie omówić te zagadnienia skrótowo. Będziemy odpowiadać na ewentualne pytania w trakcie dyskusji.

Przypomnę, że „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" ma za zadanie realizację pięciu celów szczegółowych. Pierwszy z nich to rozwój krajowego systemu cyberbezpieczeństwa. Drugim jest podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. Kolejnym celem jest zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa. Cel szczegółowy czwarty to budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństw. Celem piątym jest zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa. Wszystkie te cele są realizowane.

W informacji są też opisane szczegółowe zadania, które zostały zrealizowane w okresie od 31 października 2019 r. do 31 października br. Chciałbym powiedzieć, że najważniejsze elementy zrealizowane w ciągu minionego roku to przede wszystkim opracowanie oraz skonsultowanie w ramach administracji rządowej planu działania na rzecz wdrożenia strategii cyberbezpieczeństwa. Przypominam, że te plany są przygotowywane i aktualizowane. Konsultacje dotyczące planu trwały od 5 czerwca do 26 sierpnia br. W planie wskazano konkretne działania, wiodące oraz współpracujące podmioty odpowiedzialne za realizację danego działania, źródła finansowania tych działań oraz mierniki pozwalające na ocenę postępów realizacji danego działania.

Utworzony też został pierwszy w Polsce sektorowy zespół cyberbezpieczeństwa przy Komisji Nadzoru Finansowego, który rozpoczął funkcjonowanie 1 lipca. Zapewnia on wsparcie w obsłudze incydentów dla podmiotów z całego sektora finansowego. Jest to bardzo ważny moment, dlatego że cały krajowy system cyberbezpieczeństwa opiera się oczywiście na trzech podstawowych zespołach reagowania na incydenty komputerowe (CSIRT), ale jednym z jego głównych, podstawowych elementów, do którego

dążymy, co znajdzie swoje odzwierciedlenie także w przepisach projektu ustawy, o którym za chwilę będę mówił, jest utworzenie sieci sektorowych zespołów CSIRT.

W tym roku, a konkretnie 2 października 2020 r., rozpoczął funkcjonowanie pierwszy w Polsce zespół ISAC, czyli centrum wymiany i analizy informacji. To centrum powstało na kolei z oddolnej inicjatywy podmiotów podsektora kolei przy bardzo silnym wsparciu ze strony Ministerstwa Infrastruktury oraz eksperckiej pomocy ze strony Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego Naukowej i Akademickiej Sieci Komputerowej (CSIRT NASK). Również w tym roku Instytut Łączności – Państwowy Instytut Badawczy uruchomił pierwsze w Polsce laboratorium oceny i certyfikacji bezpieczeństwa produktów i usług na zgodność z normą *common criteria* w ramach realizacji projektu „Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria" (KSO3C). Ponadto opracowano standardy cyberbezpieczeństwa chmur obliczeniowych (SCCO) w ramach NSC, które zostały opublikowane w lutym br. przez Departament Cyberbezpieczeństwa dawnego Ministerstwa Cyfryzacji. Przygotowane także zostały założenia do realizacji przez KPRM kampanii #CyberbezpiecznySamorząd, która ma na celu wsparcie jednostek samorządu terytorialnego w obszarze podnoszenia wiedzy oraz kompetencji. Ministerstwo Obrony Narodowej kontynuowało prace związane z rozwojem Wojsk Obrony Cyberprzestrzeni. Trwa także wdrażanie unijnego zestawu środków strategicznych, technicznych i wspierających, harmonizujących na poziomie Unii Europejskiej bezpieczeństwo technologii mobilnej piątej generacji (5G), czyli tzw. *5G Toolbox*.

Ponadto, tak jak już wspominałem, przygotowany został projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i ustawy – Prawo zamówień publicznych. Projekt zakłada w pierwszej kolejności rozbudowę krajowego systemu cyberbezpieczeństwa poprzez umożliwienie tworzenia centrów ISAC, takich jak ten kolejowy, instytucjonalizację operacyjnych centrów bezpieczeństwa, czyli SOC, jak również wsparcie jednostek samorządu terytorialnego. Do systemu dodani zostaną także przedsiębiorcy komunikacji elektronicznej w zakresie wymogów bezpieczeństwa sieci i usług oraz zgłaszania incydentów, co m.in. umożliwi wdrożenie dyrektywy ustanawiającej europejski kodeks łączności elektronicznej (EKŁE). Wprowadzona zostanie możliwość oceny ryzyka dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Sektorowe zespoły CSIRT staną się obowiązkowe. Dotychczas były tylko potencjalną możliwością organów właściwych. Będzie także możliwe wydawanie ostrzeżeń oraz poleceń zabezpieczających na czas reakcji na incydent krytyczny. Projekt ustawy jest obecnie w ostatniej fazie po etapie uzgodnień międzyresortowych i konsultacji publicznych. Mamy nadzieję, że zostanie on skierowany pod obrady komitetów Rady Ministrów na początku roku.

Jeśli chodzi o realizację prac nad NSC, to trzeba przypomnieć, że chodzi tutaj o standardy i tzw. dobre praktyki w dziedzinie cyberbezpieczeństwa. W tym obszarze rozpoczęliśmy tak naprawdę prace. Chcemy, żeby te standardy miały charakter zbioru różnego rodzaju rekomendacji, które będą wdrażane w poszczególnych obszarach. Pierwszą rekomendacją, która została przez nas przyjęta, są standardy dotyczące cyberbezpieczeństwa chmury obliczeniowej, które stanowiły wkład do uchwały Rady Ministrów w sprawie inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (WIIP). W tej chwili w przygotowaniu mamy kilkanaście podobnych, choć oczywiście różnej rangi, dokumentów, które szczegółowo będą regulować poszczególne obszary.

Należy tutaj podkreślić, że jednym z elementów, który w naszym przekonaniu umożliwia nam dobrą realizację tej strategii, jest bardzo silna i dobra współpraca z sektorem przedsiębiorców, z rynkiem, może nawet przede wszystkim z producentami w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber). Do tego porozumienia przystąpiło już kilkanaście podmiotów. Dzięki tej współpracy możemy implementować cały szereg rozwiązań, które sprawdziły się zarówno w biznesie, jak i w innych państwach, z którymi współpracujemy na bieżąco.

To tyle może wprowadzenia do tematu, dlatego że nie chcę powtarzać tych informacji, które są zawarte w dokumentach. Tak jak powiedziałem, jesteśmy do dyspozycji, jeżeli ze strony Wysokiej Komisji są czy będą pytania. Dziękuję bardzo.

**Przewodniczący poseł Jan Grabiec (KO):**

Bardzo dziękuję, panie ministrze. Otwieram dyskusję. Bardzo proszę o zgłoszenia państwa posłów członków Komisji. Bardzo proszę, panie pośle.

**Poseł Krzysztof Gawkowski (Lewica):**

Dzień dobry, panie przewodniczący. Dzień dobry, panie ministrze. Chciałbym zadać dwa szczegółowe pytania i poprosić pana ministra o odpowiedź. Byłoby mi nawet bardzo miło, gdybym na pierwsze z nich otrzymał odpowiedź na piśmie i nie musiał pisać interpelacji.

Po pierwsze, chciałbym zapytać o program #CyberbezpiecznySamorząd. Czy pan minister mógłby przedstawić, jakie były jego założenia? Jak wyglądała konsultacja? Jaki jest obecny etap wdrożenia? Jak wygląda responsywność ze strony samorządów? Jaka jest informacja o wsparciu, które zostało udzielone? Jak samorządy dzięki temu programowi informują albo zwracają uwagę, że zostały wprowadzone na wyższy stopień bezpieczeństwa cybernetycznego? To jest pierwsze pytanie.

Panie ministrze, zaciekawiłem się tym, co pan powiedział, że przygotowujecie, jesteście w trakcie przygotowania, pracujecie. Forma oczywiście tutaj jest dowolna. Chodzi o standardy dotyczące cyberbezpieczeństwa. Powiedział pan, że standardy w chmurze obliczeniowej okazały się strzałem w dziesiątkę, więc bardzo prosiłbym, aby pan minister mógł opowiedzieć, jakie są inne dokumenty, które są dzisiaj przygotowywane. Nie chodzi o szczegóły. Chciałbym znać tytuły, żeby wiedzieć, jakie są kierunki dla poszczególnych obszarów i to mi wystarczy.

Gdyby na to drugie pytanie udało się też pisemnie odpowiedzieć, oprócz tego, że dzisiaj też będę bardzo wdzięczny… Prawdopodobnie, jak pan minister wystąpi z informacją o tych standardach w poszczególnych tematach, to też rozszerzę swoje pytanie i w formie interpelacji będę chciał zapytać, jakie obszarowo będą to działania, tak jak w przypadku chmury obliczeniowej. Dziękuję ślicznie.

**Przewodniczący poseł Jan Grabiec (KO):**

Dziękuję bardzo. Panie ministrze, zechce pan od razu odpowiedzieć? Bardzo proszę.

**Sekretarz stanu w KPRM Marek Zagórski:**

Tak, oczywiście. Przekażemy szczegółową odpowiedź na piśmie, zwłaszcza na to pierwsze pytanie, ale chcę też powiedzieć, że celem tego programu jest wsparcie jednostek samorządu terytorialnego przede wszystkim w zakresie podnoszenia wiedzy, ale także kompetencji. Przygotowaliśmy poradnik dla samorządów i szykujemy szkolenia. Zresztą te szkolenia się już odbywają. Myślę, ze poproszę pana dyrektora o to, żeby opowiedział więcej.

**Poseł Krzysztof Gawkowski (Lewica):**

A można od razu dopytywać?

**Sekretarz stanu w KPRM Marek Zagórski:**

Tak.

**Poseł Krzysztof Gawkowski (Lewica):**

To będę dopytywał, żebyśmy nie tworzyli później takiej dyskusji… To dobrowolne zgłoszenie czy jest jakiś system zgłaszania do tego?

**Sekretarz stanu w KPRM Marek Zagórski:**

Zgłoszenia są dobrowolne. Zaraz poproszę pana dyrektora, żeby opowiedział szczegółowo o tych szkoleniach, które się odbyły w poszczególnych województwach. Co do zasady chcemy szkolić, ale nie możemy tutaj przymusić samorządów do tego, żeby to realizowały.

Punktem wyjścia do tych działań, które podjęliśmy, były zdarzenia, które miały miejsce w kilku gminach w Polsce, kiedy doszło do zablokowania systemów przez poszczególne podmioty. Analiza, której dokonał NASK, dotyczyła bezpieczeństwa witryn internetowych, czyli stron samorządów. Wtedy okazało się, że – mówiąc bardzo delikatnie – dalekie jest ono od doskonałości. Tak bym to ujął. Podjęliśmy więc takie działania, których celem jest po pierwsze… To jest nasza ambicja. Ona dotyczy samorządów, ale także i generalnie całej administracji. Z podstawowych zasad cyberhigieny chcemy prze-

szkolić jak największą rzeszę urzędników i jak największą rzeszę samorządów. To jest pierwszy poziom.

Drugi element, który jest bardzo ważny, jest związany ze standardami cyberbezpieczeństwa i chmur obliczeniowych. Chcemy namawiać samorządy do tego, żeby korzystały z rozwiązań chmurowych, dlatego że w ten sposób będą w stanie uzyskać większą odporność na zagrożenia niż w większości przypadków są w stanie zrealizować to samodzielnie. Chcemy także podnosić kompetencje kadry, która jest odpowiedzialna za cyberbezpieczeństwo w większych jednostkach, które mają ambicje i możliwości do tego, żeby zapewniać sobie te rozwiązania w sposób samodzielny. Przy czym tutaj to nie ma tak naprawdę większej różnicy, czy mówimy o jednostkach samorządu terytorialnego, czy mówimy w ogóle o administracji wyższego szczebla, dlatego że podstawowym elementem jest określenie standardów nie tylko oczywiście chmur obliczeniowych, ale w ogóle standardów bezpieczeństwa systemów. Natomiast generalnie chodzi nam o to, żeby samorząd w tym przypadku miał pełną świadomość tego, że jest tak naprawdę włączony w cały krajowy system cyberbezpieczeństwa i że ma swoje obowiązki w tym zakresie, bo ta świadomość też bywa różna. Jak mówię, są przykłady takich gmin jak choćby Kościerzyna czy Lututów, gdzie okazało się, że świadomość na temat tego, w jaki sposób postępować – nie tylko w jaki sposób się zabezpieczać, ale nawet jak postępować w przypadku ataków – była niska. Stąd szkolenia w tym zakresie. Myślę, że pan dyrektor trochę więcej powie o tym, ile osób już zostało przeszkolonych.

Natomiast jeśli chodzi o standardy cyberbezpieczeństwa dla chmur obliczeniowych, to był w ogóle wymóg, który narzuciliśmy sobie trochę wewnętrznie jako administracja. Wynika to z tego, że nasze podejście do tego, jak przenosić administrację do chmury, bazuje na podziale systemów na dwie kategorie. Chcemy, żeby systemy – nazwijmy to bardzo umownie – wrażliwe, czyli o wyższym poziomie wrażliwości, które powinny mieć podwyższony poziom bezpieczeństwa, docelowo były w chmurze, ale rządowej chmurze obliczeniowej. Drugi obszar to są te systemy, które mogą wykorzystywać usługi chmury publicznej. Jednym z warunków było określenie i zdefiniowanie wymagań w zakresie standardów właśnie dla tych chmur obliczeniowych, z których administracja, jak np. jednostki samorządu terytorialnego, może korzystać. Zdefiniowanie tego pozwoliło nam też na to, że już w tej chwili na platformie, która się nazywa ZUCH, czyli System Zapewnianie Usług Chmurowych, mamy pierwsze podmioty, które z jednej strony oferują usługi chmurowe dla administracji, w tym dla samorządów, a z drugiej strony mamy takie podmioty, w tym jednostki samorządu terytorialnego, które już nawiązują kontakty poprzez tę platformę. Mamy nadzieję, że za chwilę dojdzie do pierwszych kontraktów i że te usługi będą realizowane.

Kolejne standardy są opracowywane na podstawie różnych dokumentów, przygotowywanych m.in. przez Agencję Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA) i przez inne organizacje. W tym materiale, który państwu przekazaliśmy, są one wyszczególnione, ale mogę powiedzieć o kilku. To chociażby zasady stosowania zabezpieczeń w systemach informatycznych dla podmiotów publicznych, ocena środków bezpieczeństwa w systemach informatycznych podmiotów publicznych, wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego czy podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego. Generalnie chodzi o to, żeby zbudować cały zasób wiedzy, który będzie dostępny w pierwszej kolejności oczywiście dla administracji, ale nie tylko, bo chodzi także o to, z czego będą mogli korzystać także przedsiębiorcy i firmy.

To tyle. Proszę pana dyrektora o uszczegółowioną informację na temat tych szkoleń, które już się odbyły w ramach kampanii #CyberbezpiecznySamorząd.

**Przewodniczący poseł Jan Grabiec (KO):**

Bardzo proszę, panie dyrektorze.

**Dyrektor Departamentu Cyberbezpieczeństwa KPRM Robert Kośla:**

Bardzo dziękuję, panie przewodniczący. Wysoka Komisjo, szkolenia z cyberbezpieczeństwa, które uruchomiliśmy w pierwszej formule, jeszcze przed pandemią, obejmowały warsztaty organizowane wspólnie z NASK w trzech województwach. Te warsztaty obejmo-

wały zarówno wprowadzenie do zagadnień teoretycznych, jak i to, w jaki sposób przygotowywać się do systemowej ochrony informacji w systemach teleinformatycznych, jak również do zwiększenia odporności systemów na ataki. Były omawiane konkretne przypadki z praktyki incydentów obsłużonych przez zespół CSIRT NASK, a w drugiej części kwestie ćwiczeń na przykładzie konkretnych sytuacji, które były omawiane na warsztatach.

Natomiast oczywiście w przypadku ograniczeń związanych z pandemią przeszliśmy na formę online. W tej chwili szkolenia są prowadzone w formie webinariów. Korzystamy w tej chwili z platformy teleinformatycznej, która umożliwia organizowanie szkoleń dla nawet do 10 tys. użytkowników w tym samym czasie. Rozsyłamy zaproszenia na kolejne edycje szkoleń w formacie webinariów. Zrobiliśmy sześć szkoleń. Dzisiaj było właśnie kolejne szkolenie. Standardowo w ramach tych szkoleń obserwujemy, że około 700 osób jednorazowo bierze udział w takim szkoleniu. Szkolenia staramy się kondensować, żeby nie zajmować więcej niż dwie godziny. Jest to wprowadzenie teoretyczne i omówienie konkretnych przypadków.

Cała informacja na temat szkoleń, jak również kampanii #CyberbezpiecznySamorząd jest na stronie. Uruchomiliśmy w ubiegłym roku dedykowaną stronę internetową na portalu gov.pl w bazie wiedzy dla przedsiębiorców, samorządów i obywateli. Strona nosi nazwę „Cyberbezpieczeństwo". W ramach tej strony są zarówno aktualności, jak i informacje dla każdego, czyli podstawowe informacje z obszaru cyberhigieny, m.in. kwestia bezpieczeństwa urządzeń mobilnych i korzystania z portali społecznościowych. Dla profesjonalistów są już konkretne zalecenia pokazujące krok po kroku, jak podnosić bezpieczeństwo systemu. Jest zakładka dedykowana samorządom.

Do dnia dzisiejszego opublikowano sześć poradników, począwszy od pierwszego poradnika, który dotyczył ochrony informacji w cyberprzestrzeni, czyli takiego wprowadzenia. Później były poradniki dotyczące zgłaszania incydentów oraz zapobiegania atakom typu *ransomware*, czyli tym atakom, z którymi mieliśmy do czynienia w przypadku Kościerzyny i Lututowa, jak postępować, jak radzić sobie w przypadku takiego ataku. Dalej był poradnik „Cyberbezpieczne usługi chmurowe dla administracji publicznej", gdzie promowaliśmy korzystanie z usług chmurowych.

Najświeższy jest poradnik „Wszystko o portalu samorzad.gov.pl", czyli promowanie usług informacyjnych dla samorządów, bo m.in. duża część samorządów, szczególnie tych najmniejszych jednostek samorządu terytorialnego, wskazywała na problemy przede wszystkim w zakresie wiedzy, jak również zasobów, z których mogą korzystać, żeby bezpiecznie uruchamiać usługi informacyjne dla obywateli. Chodzi o hostowanie swoich usług i swoich serwisów. Podczas analiz po atakach na Kościerzynę i Lututów zidentyfikowaliśmy pięć podstawowych usług, które są świadczone w systemach informatycznych samorządu terytorialnego. Są to usługi związane m.in. z obsługą podatków, wypłacaniem świadczeń społecznych. Okazało się, że lista tych pięciu usług jest wspólna, więc w tej chwili to promujemy i w ramach szkoleń organizowanych dla samorządów pokazujemy, w jaki sposób te samorządy, które są zainteresowane, mogą przenosić, migrować swoje zasoby informacyjne do platformy samorzad.gov.pl, która bazuje na tych samych rozwiązaniach technicznych, jakie zostały zastosowane przy platformie gov.pl, gdzie przenoszono wszystkie serwisy informacyjne administracji rządowej na jedną, jednolitą platformę, która jest zabezpieczana w sposób systemowy.

Oprócz tego na platformie gov.pl w bazie wiedzy „Cyberbezpieczeństwo" są informacje o szkoleniach. Jest wymieniona tematyka tych szkoleń. Są tam również umieszczane poradniki od partnerów technologicznych. Pan minister mówił o programie PWCyber, który zainicjowaliśmy. Jest to unikatowy program w Europie, który dotyczy współpracy z dostawcami technologii i z dostawcami usług, z polskimi firmami, które opracowują rozwiązania kryptograficzne i które przygotowują rozwiązania dla bezpieczeństwa przemysłu. To jest program bazujący na formacie partnerstwa. W ramach tego programu firmy przekazują rekomendacje i najlepsze praktyki, jak również informacje o wektorach i metodach ataków, które w tej chwili są najpopularniejsze, obserwując to w swojej globalnej działalności. Na tym portalu umieszczamy też poradniki dla administratorów, w jaki sposób bezpiecznie korzystać… W tej chwili mamy w opracowaniu kolejną serię poradników.

Jest również możliwość subskrypcji tych informacji, więc zachęcamy. Wysyłamy do samorządów informacje kanałem, który był wykorzystywany wcześniej przy szkoleniach z usług świadczonych dla samorządów, jak chociażby w kwestii e-dowodu czy innych usług elektronicznych, cyfrowych, do których samorządy mają dostęp. Korzystamy z tego kanału komunikacyjnego, ale uruchomiliśmy również kanał subskrypcji informacji dla obywateli, jak i dla samorządów. Mamy też sekcję dotyczącą najczęściej zadawanych pytań, gdzie można uzyskać informację na temat tego, jak podchodzić do bezpieczeństwa, jakie główne kwestie są związane z bezpieczeństwem.

Jeżeli chodzi o strukturę dokumentów NSC, to ta struktura została opracowana i wstępnie ujęta w strategii cyberbezpieczeństwa. Obejmuje ona w tej chwili osiem obszarów. To obszary zarządzania procesami cyberbezpieczeństwa, standardów technicznych dla urządzeń mobilnych i stacjonarnych, standardów konfiguracji systemów operacyjnych, standardów bezpieczeństwa aplikacji, chmur obliczeniowych i sieci, standardów kryptograficznych oraz standardów usług cyberbezpieczeństwa. W tej chwili mamy 17 dokumentów, nad którymi praca została już zakończona.

Jak pan minister mówił, w dużej części wykorzystywaliśmy dokumenty agencji ENISA, dokumenty europejskie, chociaż tych dokumentów jest w tej chwili bardzo mała liczba. Państwa członkowskie wraz z formatem, wraz z przyjęciem aktu o cyberbezpieczeństwie… Wspólnie z Europejskim Instytutem Norm Telekomunikacyjnych (ETSI) ENISA ma bardziej zaangażować się w wypracowywanie europejskich standardów. Zresztą nie ma europejskich standardów chmurowych. Polska, Niemcy i Wielka Brytania, a wcześniej Francja, to są te państwa, które mają wypracowane standardy chmurowe, więc jesteśmy tutaj jednym z liderów. Przyszłe standardy chmurowe będą bazowały również na naszym doświadczeniu.

A jeśli chodzi o doświadczenie, które zdobywamy, sięgaliśmy też po przykłady z innych państw. Rozmawialiśmy z amerykańskim Narodowym Instytutem Standaryzacji i Technologii, czyli NIST. Inspirujemy się trochę tamtym formatem, dlatego że tam standardy powstają we współpracy z przemysłem i wspólnie wypracowywane są najlepsze rozwiązania, jak również jest pełen przegląd tego, co na rynku będzie dostępne w ciągu roku czy 2–3 lat, co znajduje swoje odzwierciedlenie w standardach. Współpracujemy również z partnerami europejskimi, z państwami grupy Trójmorza. Zidentyfikowaliśmy te obszary, gdzie wspólnie będziemy działali nad rozwojem standardów regionalnych. To są te informacje, które chciałem państwu przekazać.

Tak jak mówię, mamy szczegółową listę tych dokumentów. One w tej chwili są w trakcie opiniowania, bo przekazaliśmy je do zaopiniowania przez partnerów programu PWCyber, żeby też oni mieli szansę spojrzenia na to z punktu widzenia przemysłu, na ile te dokumenty mają swoje odzwierciedlenie w praktyce.

Druga rzecz to jest kwestia wprowadzania. Na razie promujemy to jako dobre praktyki, natomiast jest oczywiście kwestia tego, w jakim zakresie i które ze standardów powinny być wprowadzone jako obowiązkowe. Tutaj prowadzimy dyskusję równolegle do prac prowadzonych na poziomie europejskim, gdzie też w ramach dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, czyli dyrektywy NIS, państwa dyskutują chociażby o tym, jakie elementy powinny być obowiązkowo certyfikowane, jakie elementy i standardy powinny być wprowadzone do wspierania bezpieczeństwa jednolitego rynku cyfrowego. Dziękuję bardzo.

**Przewodniczący poseł Jan Grabiec (KO):**

Dziękuję, panie dyrektorze. Bardzo proszę, pan przewodniczący Grzegorz Napieralski. Proszę, panie pośle.

**Poseł Grzegorz Napieralski (KO):**

Bardzo dziękuję, panie przewodniczący. Panie ministrze i panie dyrektorze, mam może trochę lżejsze pytanie, ale być może to się też dzieje. Nie wiem. Jeżeli dzieje się, to już nie wymagam.

Pytam o to, czy współpracujecie z Ministerstwem Edukacji Narodowej, żeby od poziomu dawnego gimnazjum przez szkołę średnią przygotować naszą młodzież rów-

nież do tego, żeby była uwrażliwiona. Wiemy, że już dzisiaj np. banki oferują młodym ludziom karty kredytowe, oczywiście takie z ograniczoną możliwością, ale to jakby presja nauki już od samego początku, bo u młodych ludzi to może być problem, żeby później nie było włamania na karty kredytowe czy na konta i nie tylko. Mieliśmy dzisiaj przecież też informację o włamaniu się na konto w portalu społecznościowym. Czy coś takiego dzieje się właśnie we współpracy, jeśli chodzi o wasz resort czy dzisiaj oddział KPRM i MEN?

**Przewodniczący poseł Jan Grabiec (KO):**

Bardzo proszę, panie ministrze.

**Sekretarz stanu w KPRM Marek Zagórski:**

Zanim odpowiem na to pytanie, chcę jeszcze tylko dopowiedzieć, odnosząc się do pytania pana przewodniczącego Gawkowskiego, jeśli chodzi o portal samorzad.gov.pl, że bardzo chcielibyśmy go polecić samorządom, bo on powstał w reakcji na naszą analizę dotyczącą niskiego poziomu bezpieczeństwa stron samorządowych. Było bardzo różnie, łącznie z tym, że niektóre gminy w ogóle nie miały praw do swoich domen, dlatego że rejestrowane były przez jakieś tam podmioty itd. Możemy powiedzieć, że kilka samorządów jest już przeniesionych na ten portal. Ważna informacja jest taka, że samorządy nie ponoszą tutaj żadnych kosztów, czyli, mówiąc krótko, mają pełną autonomię, jeśli chodzi o treści, natomiast mają zapewniony standard usługi na takim poziomie, jak odpowiednio ministerstwa na gov.pl. To mniej więcej taki sam mechanizm.

Wracając natomiast do pytania, chcę powiedzieć, że po pierwsze, w ramach działania 3.4 w ramach programu operacyjnego „Polska cyfrowa" realizujemy taki projekt, który się nazywa „Kampanie edukacyjno-informacyjne na rzecz upowszechniania korzyści z wykorzystywania technologii cyfrowych". W ramach jednej z tych kampanii jest kampania dotycząca cyberbezpieczeństwa czy cyberzagrożeń. To działanie prowadzimy wspólnie z NASK. Ono jest także powiązane z kwestiami bezpieczeństwa w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE). Wśród tych działań, które są prowadzone na dużą skalę, mamy zagadnienia związane w ogóle z całą kategorią cyberzagrożeń. Nie wiem, jak to zabrzmi, ale powiedziałbym, że adresatami czy odbiorcami tych cyberzagrożeń są dzieci i młodzież. Prowadzimy bardzo dużą liczbę działań różnego rodzaju – od komunikacji medialnej poprzez media społecznościowe i portale informacyjne w sieci, a także poprzez webinaria, które są adresowane do nauczycieli i do rodziców. Jednym z ambasadorów tego obszaru związanego z kwestiami zagrożeń w sieci jest m.in. Tomasz Rożek. Te webinaria cieszą się bardzo dużym powodzeniem.

Materiały edukacyjne są umieszczone m.in. na portalu OSE IT Szkoła. To jest portal prowadzony przez NASK – operatora OSE. Tam są także materiały umieszczone przede wszystkim z uwagi na specyfikę i doświadczenia NASK jako podmiotu, który specjalizuje się w zakresie cyberbezpieczeństwa i jednocześnie, łącząc te dwie funkcje, prowadzi cały szereg kampanii informacyjnych i edukacyjnych, przygotowuje materiały, których odbiorcami są i uczniowie, i nauczyciele, a także rodzice, więc cały ten proces jest prowadzony.

Tak się podzieliśmy między ministrem odpowiedzialnym za edukację a ministrem odpowiedzialnym za informatyzację, że w procesie dostarczania narzędzi i materiałów edukacyjnych po naszej stronie są kwestie związane z przygotowywaniem materiałów dotyczących bezpieczeństwa w szeroko rozumianej sieci. Te działania prowadzimy i będziemy prowadzić. W nowej perspektywie finansowej przygotowujemy też zresztą specjalną oś dotyczącą kompetencji cyfrowych i cyberbezpieczeństwa. To jest też jeden z elementów, w którym kwestie związane ze świadomością cyberzagrożeń będą bardzo mocno obecne. W dalszym ciągu będziemy je budować i będzie to kontynuowane. Plus sama OSE jako sieć z jednej strony jest tak zbudowana, żeby zapewnić odpowiedni poziom bezpieczeństwa, ale także na poziomie czwartym w ramach OSE jest przewidziane dostarczenie aplikacji nie tylko dla szkół, ale także potencjalnie dla rodziców.

**Poseł Grzegorz Napieralski (KO):**

Mogę o jeszcze jedno dopytać?

**Przewodniczący poseł Jan Grabiec (KO):**

To może tak *ad vocem*, jeśli pan poseł pozwoli.

**Poseł Grzegorz Napieralski (KO):**

Mogę, tak? Może nawet nie *ad vocem*, ale jakby uzupełnię. A nie myśleliście, panie ministrze, o czymś takim? Tak jak zrozumiałem pańską odpowiedź, dzisiaj w ramach różnych programów i takich projektów, które realizujecie, jest zawarta edukacja nie tylko młodych ludzi, ale również nauczycieli i nawet rodziców. To raczej jest rola MEN, ale spytam, czy nie myśleliście, żeby przy waszej współpracy coś takiego, co nie byłoby związane z programami bądź z różnymi akcjami informacyjnymi, jednak zostało wpisane do podstawy programowej, jeżeli chodzi o nauczanie młodych ludzi. Jeśli świat cyfrowy będzie nas coraz bardziej absorbował, będzie się coraz bardziej rozrastał i kolejne pokolenia młodych ludzi będą w nim funkcjonować, to tak jak kiedyś uczyliśmy się, że nie wolno przechodzić na czerwonym świetle, bo ktoś może nas przejechać, tak dzisiaj musimy się uczyć właśnie takich kompetencji, żeby ktoś nam nie włamał się do telefonu i nie zrobił nam krzywdy. Mówię oczywiście w dużym uproszczeniu, ale myślę, że pan minister to zrozumiał. Dziękuję bardzo.

**Sekretarz stanu w KPRM Marek Zagórski:**

Nie tylko to rozumiem, ale taką inicjatywę podjęliśmy i w planie działań właśnie w strategii jest to przewidziane. Z jednej strony dobrze jest rzeczywiście dyskutować o wprowadzeniu tego typu elementów do podstawy programowej, a z drugiej strony na takich zajęciach jak chociażby wiedza o społeczeństwie te elementy są już od jakiegoś czasu. W dużej mierze to jest związane nie tylko z kwestią wprowadzenia do podstawy programowej, ale także z podnoszeniem kompetencji samych nauczycieli w tym zakresie, co też realizujemy i musi to iść w parze. Tak, ale jest to przewidziane.

**Przewodniczący poseł Jan Grabiec (KO):**

Bardzo proszę, pan poseł Robert Kwiatkowski. Chyba trzeba pinezki użyć, jeśli legitymacji nie ma pan pod ręką. Panie pośle, wystarczy z lewej strony. Bardzo proszę.

**Poseł Robert Kwiatkowski (Lewica):**

Jest, udało się. Pytanie jest banalne. Dotyczy strategii cyberbezpieczeństwa. Czy uwzględniony jest trzeci sektor? Nie znalazłem nigdzie zapisów dotyczących różnego rodzaju organizacji pozarządowych w tej narodowej strategii cyberbezpieczeństwa. Być może to wynika ze zbyt pobieżnej lektury.

Drugie pytanie dotyczy – powiedzmy – sektora *for-profit*. Rozumiem, że pracujecie z różnego rodzaju przedsiębiorcami. Mam na myśli nie tyle przedsiębiorców i operatorów telekomunikacyjnych, operatorów sieci itd., tylko – w cudzysłowie – normalne firmy spoza sektora IT. Rozumiem, że jakoś z nimi pracujecie, bo wzmiankę na ten temat znalazłem. Czy jest jednak jakaś wewnętrzna gradacja wrażliwości poszczególnych przedsiębiorstw czy sektorów gospodarki z punktu widzenia cyberbezpieczeństwa? Dziękuję.

**Przewodniczący poseł Jan Grabiec (KO):**

Bardzo proszę, panie ministrze.

**Sekretarz stanu w KPRM Marek Zagórski:**

Po pierwsze, jeśli chodzi o trzeci sektor, oczywiście współpracujemy i chcemy, żeby ta współpraca była podnoszona na jeszcze wyższy poziom. Na przestrzeni ostatnich kilkunastu dni rozmawialiśmy także na temat usystematyzowania tej współpracy chociażby z takimi podmiotami, które są bardzo aktywne w sieci. Nie chcę teraz wymieniać, bo nie mamy tego jeszcze do końca potwierdzonego, ale planujemy taką formułę współpracy z najbardziej znanymi portalami czy organizacjami, które zajmują się cyberbezpieczeństwem w sieci. Chcemy je mocniej włączyć we współpracę zgodnie z filozofią, którą przyjęliśmy jeszcze w Ministerstwie Cyfryzacji, że pracujemy w różnych obszarach w ramach grup roboczych z różnymi podmiotami, zarówno z biznesem, jak i z trzecim sektorem, a także ze środowiskiem naukowym. Takim sektorem naturalnym jest także cyberbezpieczeństwo i funkcjonuje grupa robocza do spraw cyberbezpieczeństwa. Natomiast chcemy, żeby specjalnie jeszcze potraktować trzeci sektor, choć to często też

są przedsiębiorstwa, które prowadzą działalność, ale są bardzo aktywne w przestrzeni społecznej. W związku z tym jak najbardziej chcemy to wykorzystać nie tylko w kwestii popularyzacji, ale także w kwestii wymiany informacji, co też jest bardzo istotne.

Jeśli chodzi natomiast o współpracę z podmiotami, czy jest jakaś gradacja i czy widzimy tutaj wszystko, staramy się widzieć wszystko. Podstawą naszej polityki w tym zakresie i tą gradacją jest oczywiście to, że na pierwszym miejscu są podmioty, które są elementem krajowego systemu cyberbezpieczeństwa. One są dla nas kluczowe, najważniejsze. Mają też one swoje obowiązki wynikające z ustawy. Często się to pokrywa z tymi podmiotami, z którymi mamy podpisane porozumienie w ramach Programu Współpracy w Cyberbezpieczeństwie, czyli PWCyber, ale nie zawsze, bo są też takie podmioty, które nie są elementami krajowego systemu cyberbezpieczeństwa, a z nami współpracują.

Kolejna grupa to są średnie i małe firmy, które m.in. zgromadzone są w #CyberMadeInPoland. Tutaj współpracujemy z Instytutem Kościuszki, który taką inicjatywę zorganizował. Chodzi o to, żeby promować także rozwiązania w zakresie cyberbezpieczeństwa generowane przez mniejsze startupy polskie i wykorzystywać także ich spojrzenie na budowę krajowego systemu cyberbezpieczeństwa. Na marginesie chcę też powiedzieć *à propos* trzeciego sektora, że jednym z podmiotów, które wchodzą w skład porozumienia PWCyber, jest Fundacja Bezpieczna Cyberprzestrzeń, która jest pierwszym z podmiotów, jakie podpisały z nami to porozumienie.

Wreszcie osobnym zagadnieniem jest kwestia naszego spojrzenia na te firmy, które nie są podmiotami branżowymi. Przede wszystkim naszą uwagę koncentrujemy na małych i średnich przedsiębiorcach, choć oczywiście także i duże przedsiębiorstwa mogą w tym uczestniczyć. Realizujemy to po pierwsze w zakresie kampanii informacyjnych dotyczących cyberzagrożeń, bo ich odbiorcami jest ogół społeczeństwa, ale także małe i średnie przedsiębiorstwa. Natomiast szczególnie chcemy na to zwrócić uwagę w nowej perspektywie finansowej, bo chcemy przygotować odpowiednie narzędzia, które będą zachęcały zwłaszcza małe i średnie firmy do kupowania rozwiązań podnoszących ich poziom bezpieczeństwa, czy to usług chmurowych, czy wprost usług w zakresie cyberbezpieczeństwa. Tutaj w ramach Krajowego Planu Odbudowy (KPO), ale także wieloletnich ram finansowych, czyli nowej wersji programu operacyjnego „Polska cyfrowa”, przewidujemy bezpośrednie wsparcie finansowe dla tej kategorii przedsiębiorstw po to, żeby mogły kupować tego typu usługi, plus oczywiście wsparcie szkoleniowe. To jakby jest odrębna, ale równie ważna kwestia, bo bez tej świadomości oni nie będą mieli potrzeby kupowania tego typu usług, więc to musi iść ze sobą w parze.

**Przewodniczący poseł Jan Grabiec (KO):**

Dziękuję bardzo, panie ministrze. Czy są jakieś pytania ze strony parlamentarzystów uczestniczących zdalnie w naszym posiedzeniu albo gości Komisji? Bardzo proszę o pytania lub głosy w dyskusji. Nie mamy takich zgłoszeń? Nie mamy.

Jeśli nie będzie zgłoszeń w tym zakresie, to uznam, że wyczerpaliśmy punkty pierwszy i drugi posiedzenia. Nie widzimy takich zgłoszeń w tej chwili. W związku z tym stwierdzam, że punkty pierwszy i drugi zostały zrealizowane.

Na tym wyczerpaliśmy porządek dzisiejszego posiedzenia. W związku z tym dziękuję państwu za udział i zamykam posiedzenie Komisji. Dziękuję bardzo, panie ministrze. Dziękuję wszystkim uczestnikom posiedzenia.